Research Paper | Computer Science | E-ISSN No : 2454-9916 | Volume : 3 | Issue : 5 | May 2017

EFFECTIVE HARDWARE ENACTMENT OF LED BLOCK CIPHER

Pushpendra Kumar Verma

Assistant Professor, Computer Science, Swami Vivekanand Subharti University, Meerut, Uttar Pradesh, India.

ABSTRACT

Resource constrained devices such as RFID and sensor nodes contain sensitive and confidential information. Such devices are used in many applications leading to an ever increasing need to provide high speed security. In order to satisfy these constraints in the small embedded applications which have limited resources, lightweight symmetric LED block cipher plays a major role in the bulk data encryption. In this paper implementation of a hardware efficient symmetric LED (Light Encryption Device) block cipher design that increasing speed using high speed parallel sub-pipelined architecture is proposed. This approach is done for block size of 128-bits and key size of 128-bits. The trade of between the low resource requirement and cryptographic strength is balanced here. It is tested by encrypting and decrypting a single 128 bit block. The algorithm was designed using VHDL. To verify the digital design at the software platform modalism simulator Altera 6.5e is used and synthesized using the Xilinx synthesizer and targeted in low cost FPGA device Spartan 6.

KEYWORDS: Lightweight cryptography, FPGA, LED Block Cipher, Security, Confidentiality.

I. INTRODUCTION:

Cryptography is an important aspect of communications security and is becoming increasingly important as a basic building block for computer security.. Cryptography began thousands of years ago. It's also found in old kingdom of Egypt circa during 1900BC.Some clay tablets from Mesopotamia are clearly meant to protect information one dated near 1500BC was found to encrypt a craftsman's recipe for pottery glaze, presumably commercially valuable. Today more and more sensitive data is stored digitally. Personal emails, bank accounts and medical records are confidential information that data must kept secure. The use of systems with more complexity, which are usually more secure, has a result low throughput rate and more energy consumption. Even though the evolution of cipher has no practical impact, it has more theoretical background. After the advent of the internet the security of data and protection of privacy have become a major concern for day to day Life, although researchers and mathematicians have been trying to address this problem since the end of the World War II, when cryptology science came out from the ambit of the army to enter the Bell Laboratories. The cryptography must ensure the tradeoff between security and low resource requirement. Information Security play an important role in our lives to satisfy the day by day life. The increase in use of computer and communication system for the data and money transfer has increased the risk of theft of information. In order to provide security there is a need of secure communication of the algorithm must ensure that fast and secure digital communication, the data is kept secret, the entity of data is preserved, the user identity is genuine [1]. Cryptography provides different algorithm for securing and authenticating the transmission of information over the channels. RFID and sensor nodes contain sensitive information and confidential information such device are used in many application but these miniature device are not possible to run in traditional cryptography which require large memory and greater power. In order to satisfy this constraint Lightweight cryptography is used. “As light as feather and hard as dragon scale” was Bilbo Baggins description for Mithril, a legendary material in J.R.R. Tolkiens famous novel “The Lord of the Rings” .The main objective of lightweight cryptography aims to yield very lightweight implementations that are virtually “light as a feather”, “Hard as dragon scales” is a good paraphrase for this aspect, because it emphasizes that there are sufficient security levels [7]. Symmetric key cryptography and asymmetric cryptography are the two types of cryptography. The Symmetric key cryptography use the same key for both encryption as well as decryption, while the counterpart Asymmetric key use a public key for encryption and a private key for decryption. The Symmetric key encryption is further classified into two types Block cipher and stream cipher. The stream cipher encrypts data bit by bit whereas the block cipher can encrypt block of data. The main operations of cryptographic algorithm are that the encryption and decryption takes place under the action of fixed block sizes called as plain text. Some of the lightweight cryptographic algorithm present today is AES, DES, HIGHT, PRESENT, KTANTAN, AND KATAN, KLEIN, PRINCE, TWINE, TEA AND XTE LED. Among all these, the LED block cipher stay ahead in terms of security even without key schedule. When compared to other existing lightweight block cipher, the LED block cipher is more resistant to classical attacks and also to the related key at In this paper, the section 2 gives an overview of LED algorithm. Section 3 gives the implementation of proposed architecture. Section 4 gives an overview of hardware implementation. Section 5 explains the various performance matrices of the algorithms.

II. LIGHT ENCRYPTION DEVICE

SPN (Substitution Permutation Network) [4] type Lightweight block cipher, which is designed by Guo et al. in 2011. It uses the key size varying from 64 bits to 128 bits. The step function is performed eight bit key and twelve times for a 128-bit provided key is used repeatedly and provides efficient advantage in hardware implementation [2]. The overview of algorithm of Light Encryption Device is shown in Figure algorithm, the steps performed in Add Round key are follows the key K=K63……K0 is EX text P=P63……..P0. In this method 128 bit key size is used. Initially the plain text is EO (k1) where k1 ranges from 0 to 63 bits of total key after the completion of rounds the OR' end, where K2 range from 64 to 127 bits of the total key size.k1 and K2 are alternatively EX every four rounds

a) S-Boxes LED lightweight block cipher makes use of a PRESENT S-box, which has been adopted by man algorithms is shown in table 1.The goal of substitution is to reduce the correlation between input and output.

b) Shift Row The shift row transformation consist of
   (i) not shifting the first row of the state array;
   (ii) The second row is circularly shifting by one byte to the left;
   (iii) The third row is circularly shifting by two bytes to the left; and
   (iv) The last row is circularly shifted the left.

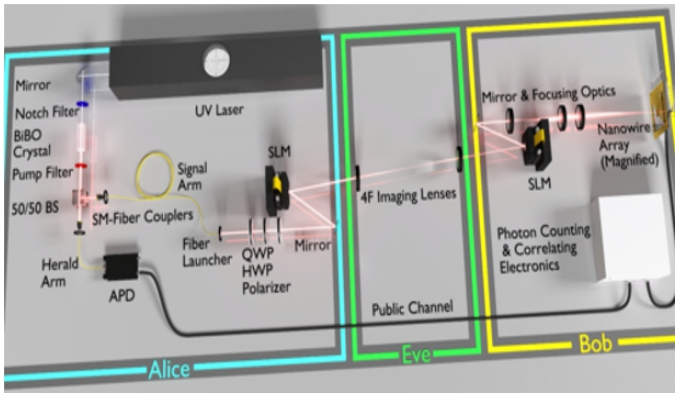


Figure1. Light Encryption Device

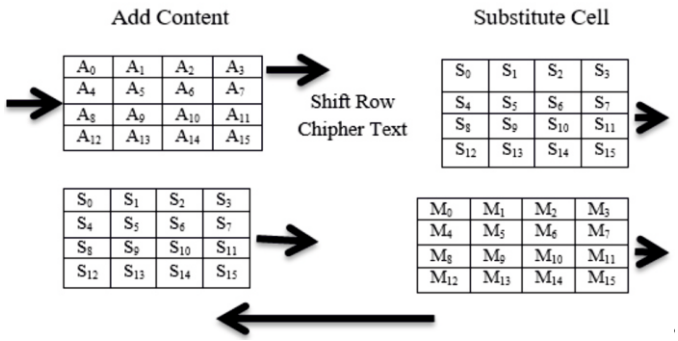
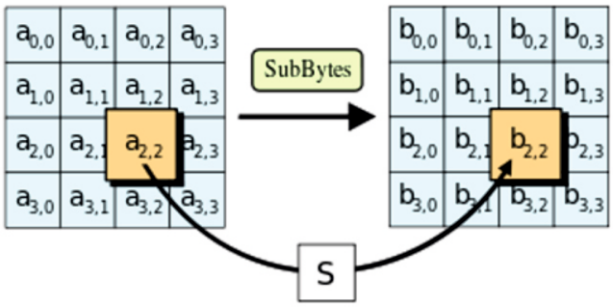


Figure2: Operation involved in LED

Table 1 S-Box

A	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

C. Mix-Column Serial Each column vector is replaced by another column vector after multiplying it with the matrix which is shown in Figure 3.



III. ENACTMENT OF LED:

The hardware implementation of LED block cipher by JianGuo, Thomas Peyrin, Axel Poschmann and Matt Robshaw has been proposed in 2011 and implemented. Lightweight Encryption method block cipher is a 64-bit block cipher that procedures cryptographic key sizes changing from 64-bits to 128 bits. Figure 4. Sub-pipelined parallel Light Encryption Device architecture It is proposed to achieve high throughput through, parallel sub pipelined architecture is shown in figure 4. In this architecture the 128-bit key is divided into 2 blocks of 64-bit and it is processed parallel. To store the intermediate values the register is inserted, it act as a buffer and they can be used for further processing. By key scheduling the 128-bit key is divided into two 64- bit blocks and processed parallel by sending to set of blocks and perform ten rounds of operation. Add Constant, Substitute cells, Shift Rows and Mix columns are the modules used for the design. In the pipelined architecture, the inputs are given to more than one round, so that more than one input can processed at a time and thereby the throughput of the architecture get increased. The throughput thus obtained is 10% more than that of loop unrolled architecture. Further to increase the throughput the sub-pipelined architecture is used. The register is used in sub-pipelined architecture among substitute cell, shift Rows and Mix-Columns to store intermediate results. Here the processing time get increased to overcome that parallel architecture is used. Thus the parallel architecture reduces the tradeoff between the area and speed.

IV. PRESENTATION METRICES:

The important parameter required for the evaluation of the implementation of this architecture are Throughput and Efficiency. The Very High Speed Hardware Description Language code is written for this architecture.

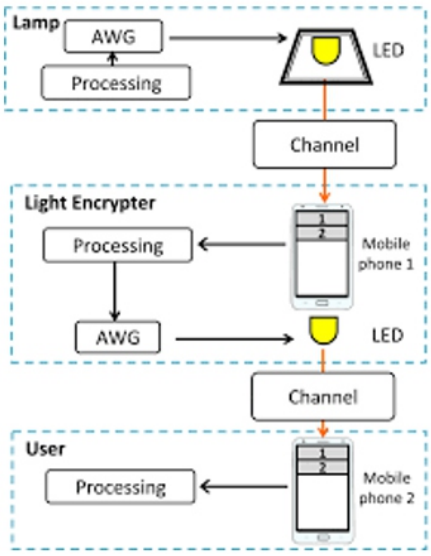


Figure 4: Parallel Light Encryption Model

Throughput and efficiency analysis the speed at which the data is encrypted and decrypted is throughput. The performance of the algorithm is mainly determined by the Throughput. The throughput [10] can be calculated by the formula

Throughput=128*Number of blocks/cycle Period

The efficiency [11] is calculated

Efficiency =Throughput /Area

Area Analysis In general, there is a tradeoff between the throughput and area. In pipeline architecture the area get increased at the cost of speed. Due to the increased number of register in between the rounds the area gets increased by sub pipelined architecture. The proposed architecture also devours more area compare to other cryptography architecture. It is necessary to shrinkage.

V. RESULT AND DISCUSSION:

The symmetric lightweight efficient LED algorithm is designed using VHDL and simulated using modalism simulator Altera 6.5e and synthesized using the Xilinx synthesizer and targeted in FPGA device Spartan 6. The modalism simulation results of LED block cipher Encryption and Decryption is shown in Figure 5 and Figure 6 respectively. In this work FPGA device SPARTAN 6 is targeted.Spartan-6 devices are the most cost-optimized FPGAs, offering industry leading connectivity features such as high logic small form-factor packaging, and a diverse number of supported I/O protocols. Built on 45nm technology, devices are ideally suited for a range of advanced bridging applications found in automotive infotainment, consumer, and industrial automation.

The algorithm is verified using the input which is shown below (in Hexadecimal representation)

Plain Text : 0123456789ABCDEF0123456789ABCDEF

KEY : 01234567898048D159E26AF37BEBCDEF

Cipher Text: 7C266E85A762BDDF7C266E85A762BDDF

VI. CONCLUSION AND FUTURE WORK:

Cryptography algorithm is omnipresent in modern communication in which the information security, such as confidentiality of communication or reliable authentication is absolute necessities. Efficient implementation techniques are necessary in order to provide high-security cryptographic algorithms.

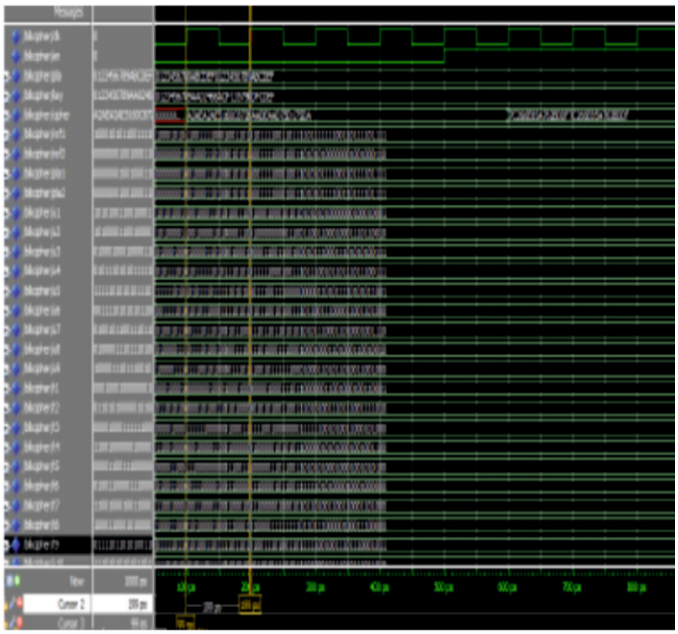


Figure 5. Simulation of encryption module

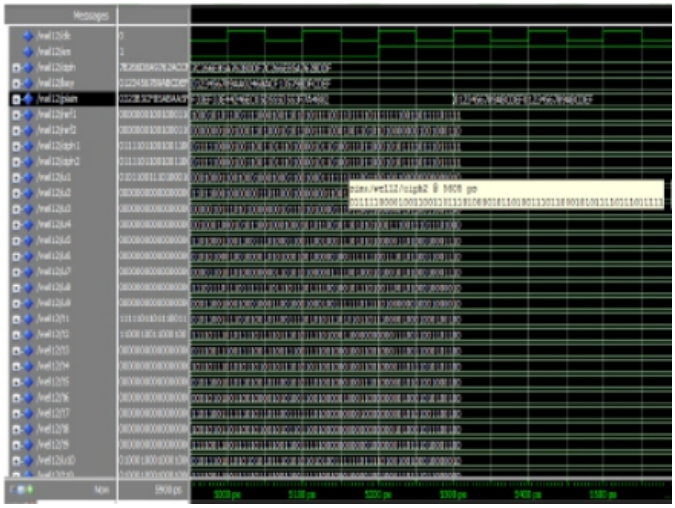


Figure 6. Simulation of decryption module

Hence in this work, encryption of serial and parallel sub-pipelined of Light-weight LED block cipher was successfully simulated using modalism simulator Altera 6.5e and synthesized using the Xilinx synthesizer and targeted in FPGA device Spartan 6.This work is mainly concentrate on the improvement of throughput of the Algorithm. Further the area of the device can be reduced by reducing the number of rounds in the algorithm

REFERENCES

[1] R. RajaRaja and D. Pavithra, "Implementation of Hardware Efficient Light Weight Encryption Method", International conference on Communication and Signal Processing, April 3-5, 2013, India, ©2013 IEEE.

[2] JianGuo, Thomas Peyrin, Axel Poschmann, and Matt Robshaw, "The LED Block Cipher", Cryptographic Hardware and Embedded Systems, Springer

[3] Mika Fujishiro , Masao Yanagisawa and NozomuTogawa "Scan-based Attack on the LED Block Cipher Using Scan Signatures",978-1-4799-3432-4/14/$31.00 ©2014 IEEE

[4] Swarnendu Jana, JaydebBhaumik, Manas Kumar Maiti "Survey on Lightweight Block Cipher",International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231 2307, Volume-3, Issue-5, November 2013

[5] National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)," Federal Information Processing Standard (FIPS) 197, 2001.

[6] J. Daemen and V. Rijmen, "The block cipher Rijndael Smart Card research and Applications, LNCS 1820, Springer-Verlag, pp. 288-296.

[7] Axel York Poschmann, "Lightweight Cryptography: Cryptographic Engineering for a pervasive world", 2009.

[8] MickaelCazorla, Kevin Marquet and and Benchmark of Lightweight Block Ciphers for Wireless Sensor Networks,"Universite de Lyon, INRIA, INSA CITI-INRIA, F-69621, Villeurbanne, France